$a({\rm mod} p)$の剰余位数の分布について (解析数論の展望と諸問題)

AUTHOR(S):

知念, 宏司; 村田, 玲音

CITATION:

知念, 宏司 ...[et al]. $a({\rm mod} p)$の剰余位数の分布について (解析数論の展望と諸問題). 数理解析研究所講究録 2001, 1219: 245-255

ISSUE DATE:

2001-07

URL:

http://hdl.handle.net/2433/41276

数理解析研究所講究録 1219 巻 2001 年 245-255

$a \pmod p$ の剰余位数の分布について

大阪府立大学　総合科学部　知念 宏司　(Koji Chinen)
College of integrated arts and sciences, Osaka Prefecture University.
明治学院大学　経済学部　村田 玲音　(Leo Murata)
Department of Mathematics, Faculty of Economics, Meijigakuin University.

1　問題とその背景

自然数 a $(a \neq 1)$ をとり, p は奇素数, $p \nmid a$ とする. また $D_a(p)$ を a の mod p での剰余位数, つまり $\mathbf{Z}/p\mathbf{Z}^\times$ において a が生成する部分群 $\langle a \rangle$ の位数, そして $I_a(p) := |\mathbf{Z}/p\mathbf{Z}^\times : \langle a \rangle|$ (a の mod p での剰余指数) とする. 次の問題を考える:

問 題 1.1 集合

$$Q_a(x;k,l) := \{p \leq x\ ;\ D_a(p) \equiv l \pmod k\} \quad (0 \leq l < k)$$

の自然密度, i.e. $\lim_{x\to\infty} \sharp Q_a(x;k,l)/\pi(x)$ を求めよ ($\pi(x)$: x 以下の素数の個数).

このような問題を考えるに到った背景について説明する. 上記の D_a, I_a はともに奇素数全体の集合 P から自然数の集合 $\mathbf{N}$ への写像を与えているが, これらが全射であるか, という問題がある. これに対し, まず D_a は, $\mathbf{N}$ から高々有限個の元を除けば全射であること, すなわち, a によって決まる有限集合 $A(a) \subset \mathbf{N}$ ($A(a) = \emptyset$ もあり得る) が存在して,

$$D_a : P \longrightarrow \mathbf{N} - A(a)$$

が全射となることが Ihara [4] によって示されている. I_a については, ある種の Kummer 拡大体 (無限個) に対する一般 Riemann 予想の仮定のもとで, a の square-free part a_1 が $a_1 \not\equiv 1 \pmod 4$ なら

$$\sharp\{p \leq x;\ I_a(p) = n\} \sim C_a^{(n)} \mathrm{li}\, x \quad (C_a^{(n)} > 0, x \to \infty) \tag{1.1}$$

となることが知られている (Lenstra [6], Murata [8]). とくに $n = 1$ の場合は, いわゆる「原始根に関する Artin の予想」で, Hooley [3] によって示されている. また $\mathrm{li}\, x = \int_2^x (1/\log t)dt$.

さて, 「全射」とは定性的な性質であるが, 定量的性質はどうであろうか. I_a については上の結果 (1.1) が解答を与えている. しかし D_a の定量的性質はほとんど知られていないと思われる. D_a と I_a には

$$D_a(p)I_a(p) = p - 1 \tag{1.2}$$

という関係があるが, 言わば $\{p-1;\ p:$ 素数 $\}$ の分布の不規則性をほとんど $D_a(p)$ の方が受け継いでいて, 挙動が不規則なため調べにくいという事情があると考えられる. そこでわれわれは, D_a の定量的性質を得るための一つの試みとして, $D_a(p)$ の値を mod k で分類することを考えた. これが問題 1.1 の背景である. もし D_a が $\mathbf{N}$ を「均等に」覆うのであれば, 上記 $Q_a(x;k,l)$ の密度はどれもだいたい $1/k$ になると期待される.

また, $a = 10$ とすれば, $D_{10}(p)$ は $1/p$ を 10 進小数展開したときの循環節の桁数に等しく, 問題 1.1 は, $1/p$ の循環節の桁数を $\bmod k$ で分類するという, きわめて初等的な意味も持つことがわかる. このうち $k = 2$ の場合は, アマチュア研究家の富澤氏が [7] において $x = 10000, 100000$ に対して $\sharp Q_{10}(x; 2, l)$ $(l = 0, 1)$ を数値実験により求め, $\lim_{x\to\infty} \sharp Q_{10}(x; 2, 0)/\pi(x) = 2/3$ を予想している.

最後に, このあと登場する記号をまとめておく. 整数 k に対し, ζ_k は 1 の原始 k 乗根, $\varphi(k)$ と $\mu(k)$ はそれぞれ Euler の関数と Möbius の関数を表す. また素数 q のべき q^e に対し, $q^e \| k$ は $q^e | k$ かつ $q^{e+1} \nmid k$ を表すものとする. そして, K を有限次代数体, $\mathfrak{p}$ を K の素イデアルとし, L/K を有限次 Galois 拡大とする. このとき Frobenius 記号 $(\mathfrak{p}, L/K)$ を

$$(\mathfrak{p}, L/K) = \left\{ \sigma \in \mathrm{Gal}(L/K) \; ; \; \begin{array}{l} \mathfrak{p} \text{ の上の } L \text{ のある素イデアル } \mathfrak{q} \text{ に対して } \mathfrak{q}^\sigma = \mathfrak{q}, \\ L \text{ の任意の整数 } \alpha \text{ に対して } \alpha^\sigma \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{q}} \end{array} \right\}$$

で定義する. ただし, $N\mathfrak{p}$ は $\mathfrak{p}$ の絶対ノルム. なお, この Frobenius 記号の記法は Lenstra [4] による.

2 主結果

主結果を述べる前に, 証明に必要な「一般 Riemann 予想 (Generalized Riemann Hypothesis, 以下 GRH)」を述べておく:

仮定 2.1 (一般 Riemann 予想) $m, k \in \mathbf{N}$, $k|m$ とする. このような任意の m, k に対し Kummer 体 $K = \mathbf{Q}(\zeta_m, a^{1/k})$ に付随する Dedekind zeta 関数 $\zeta_K(s)$ の非自明な零点は, すべて $\mathrm{Re}\, s = 1/2$ 上にある.

以下が今回の主結果である. 2 種類の結果を紹介する. まず素数を法として $D_a(p)$ を分類することを考える:

定理 2.2 $a \in \mathbf{N}$, square-free, $a > 2$, q: 素数とすると,

$$\sharp Q_a(x; q, 0) = \frac{q}{q^2 - 1} \mathrm{li}\, x + O\left(\frac{x}{\log x \log\log x} \right) \quad (x \to \infty).$$

次に mod 4 での分類を考える. (ii) の証明に GRH が必要である:

定理 2.3 a は定理 2.2 の通りとする.
(i) $l = 0, 2$ のとき

$$\sharp Q_a(x; 4, l) = \frac{1}{3} \mathrm{li}\, x + O\left(\frac{x}{\log x \log\log x} \right) \quad (x \to \infty).$$

(ii) さらに $a \equiv 1 \pmod 4$ を仮定する. $l = 1, 3$ のとき, GRH の仮定のもとで,

$$\sharp Q_a(x; 4, l) = \frac{1}{6} \mathrm{li}\, x + O\left(\frac{x}{\log x (\log\log x)^{5/2}} \right) \quad (x \to \infty).$$

このように, $Q_a(x; k, l)$ の密度は $1/k$ づつではないのである. また, 定理 2.2 と定理 2.3 (i) は何も仮定せずに証明できるが, 定理 2.3 (ii) は現状では GRH が必要である.

3 証明の概略 (1) — unconditional cases

ここでは定理 2.2 の証明を述べる. 定理 2.3 の (i) もほぼ同様である.

一般に, a を固定して p を動かしたときの D_a の動きはきわめて不規則であるが, これを I_a の言葉で書き換えると, 代数体に関する量を用いて, ある程度挙動を知ることができる. D_a から I_a への移行は, 一種の sieve method による. 式 (1.2) より, $D_a \equiv 0 \pmod q$ であるためには $q|p-1$ が必要. そこで $q^j||p-1$ なる p を考える ($j \geq 1$). この条件のもとでは

$$q|D_a \quad \Leftrightarrow \quad q^j \nmid I_a$$

なので,

$$Q_a(x;q,0) = \bigcup_{j=1}^{\infty} \{p \leq x;\ p \equiv 1 \pmod{q^j},\ p \not\equiv 1 \pmod{q^{j+1}},\ q^j \nmid I_a\}, \quad \text{(disjoint)}$$

したがって

$$\begin{aligned} \sharp Q_a(x;q,0) &= \sharp\{p \leq x;\ p \equiv 1 \pmod q\} \\ &- \sum_{j=1}^{\infty} \sharp\{p \leq x;\ p \equiv 1 \pmod{q^j},\ q^j|I_a\} \\ &+ \sum_{j=1}^{\infty} \sharp\{p \leq x;\ p \equiv 1 \pmod{q^{j+1}},\ q^j|I_a\}. \end{aligned} \tag{3.1}$$

式 (3.1) 右辺 1 行目は算術級数中の素数集合なので, 算術級数定理 (Siegel-Walfisz の定理) により自然密度がわかる:

$$\sharp\{p \leq x;\ p \equiv 1 \pmod q\} = \frac{1}{\varphi(q)} \left\{ \operatorname{li} x + O\left(x e^{-c\sqrt{\log x}} \right) \right\} \quad (c > 0).$$

そこで第 2 行の和について考えよう (第 3 行も同じである). 簡単のため,

$$(\text{右辺第 2 行の和}) = \sum_{j=1}^{\infty} \sharp M_j(x), \quad M_j(x) := \{p \leq x;\ p \equiv 1 \pmod{q^j},\ q^j|I_a\}$$

とおく. まず, x を十分大として固定すれば, 上の和は実質的には有限和である. 実際, $q^j > x$ なら $p \equiv 1 \pmod{q^j}$ は成立しないので $M_j(x) = \emptyset$ となるから, $q^j \leq x$ まで加えれば十分である. ここで区間 $(0,x]$ を 3 つに分ける:

$$(0,x] = I_1 \cup I_2 \cup I_3,$$

$$I_1 = (0, \log\log x], \quad I_2 = (\log\log x, x^{1/2}\log^2 x], \quad I_3 = (x^{1/2}\log^2 x, x].$$

すると

$$\sum_{j=1}^{\infty} \sharp M_j(x) = \left(\sum_{q^j \in I_1} + \sum_{q^j \in I_2} + \sum_{q^j \in I_3} \right) \sharp M_j(x).$$

区間 I_3 上の和については, Hooley [1] の (3) 式と全く同様に,

$$\sum_{q^j \in I_3} \sharp M_j(x) = O\left(\frac{x}{\log^3 x}\right) \tag{3.2}$$

が示される. 区間 I_2 上の和については (これも Hooley と同様だが),

$$\begin{aligned} \sharp M_j(x) &\leq \sharp\{p \leq x;\ p \equiv 1 \pmod{q^j}\} \\ &= \frac{1}{\varphi(q^j)}\left\{\operatorname{li} x + O\left(xe^{-c\sqrt{\log x}}\right)\right\} \end{aligned}$$

(Siegel-Walfisz) によって評価すると,

$$\sum_{q^j \in I_2} \sharp M_j(x) = O\left(\frac{x}{\log x \log\log x}\right) \tag{3.3}$$

となる. 最後に区間 I_1 上の和を評価しよう. 次のことを利用する:

補 題 3.1 $0 \leq j \leq i$ のとき,

$$p \equiv 1 \pmod{q^i} \text{ かつ } q^j | I_a \quad \Leftrightarrow \quad p \text{ は } K_{i,j} := \mathbf{Q}(\zeta_{q^i}, a^{1/q^j}) \text{ で完全分解する.}$$

さて, p が $K_{i,j}$ で完全分解するとき, p の上にある $K_{i,j}$ の素イデアルはちょうど $[K_{i,j} : \mathbf{Q}]$ 個である. そのような素イデアル $\mathfrak{p}$ について $N\mathfrak{p} = p$ であることに注意すれば,

$$\sharp M_j(x) = \frac{1}{[K_{j,j} : \mathbf{Q}]}\pi^{(1)}(x, K_{j,j}), \tag{3.4}$$

ただし

$$\pi^{(1)}(x, K) = \sharp\{\mathfrak{p} :\ K \text{ の 1 次の素イデアル, } K \text{ で不分岐, } N\mathfrak{p} \leq x\}.$$

これは代数体の素イデアル定理を用いて評価できる:

定 理 3.2 $K = K_{i,j}$ $(0 \leq j \leq i)$, $n = [K_{i,j} : \mathbf{Q}]$, Δ を K の判別式とし,

$$\pi(x, K) := \sharp\{\mathfrak{p} : K \text{ の素イデアル, } N\mathfrak{p} \leq x\}$$

とすれば, $e^{10n(\log|\Delta|)^2} \leq x$ のとき,

$$\pi(x, K) = \operatorname{li} x + O\left(xe^{-d\frac{\sqrt{\log x}}{n^2}}\right).$$

ただし, d および O の含む定数は n によらない.

証 明 Lagarias-Odlyzko [3] の Theorems 1.3, 1.4 による. $K = K_{i,j}$ に対しては $|\Delta| \leq (n^2|a|)^n$ という評価が成り立つので, 上の形となる. ∎

この定理は一般 Riemann 予想などの仮定を必要とせず, 無条件で成り立つ定理である. 2 次以上の素イデアル, および K で分岐する素イデアルの寄与を評価すれば, 次が得られる:

$$\pi^{(1)}(x, K_{i,j}) = \operatorname{li} x + O\left(nxe^{-d\frac{\sqrt{\log x}}{n^2}}\right) \qquad (e^{10n(\log|\Delta|)^2} \leq x). \tag{3.5}$$

拡大次数 $n_j := [k_{j,j} : \mathbf{Q}]$ については, $n_j = q^{2j-1}(q-1)$ が知られているから (Moree [5, Lemma 2] または Murata [6, Section 3]), (3.4) と (3.5) から,

$$\begin{aligned}\sum_{q^j \in I_1} \sharp M_j(x) &= \sum_{q^j \in I_1} \left\{\frac{1}{n_j}\operatorname{li} x + O\left(xe^{-d\frac{\sqrt{\log x}}{n_j^2}}\right)\right\} \\ &= \left(\sum_{j=1}^{\infty}\frac{1}{n_j} - \sum_{q^j > \log\log x}\frac{1}{n_j}\right)\operatorname{li} x + O\left(\sum_{q^j \in I_1} xe^{-d\frac{\sqrt{\log x}}{n_j^2}}\right).\end{aligned}$$

これらのうち

$$\sum_{q^j > \log\log x} \frac{\operatorname{li} x}{n_j} = O\left(\frac{x}{\log x(\log\log x)^2}\right),$$

$$\sum_{q^j \in I_1} xe^{-d\frac{\sqrt{\log x}}{n^2}} = O\left(\frac{x}{\log^N x}\right) \quad (\forall N \geq 1)$$

および (3.2), (3.3) はいずれも $\operatorname{li} x \sim x/\log x$ より小さいので, これらを剰余項としてまとめれば,

$$\sum_{j \geq 1} \sharp M_j(x) = \sum_{j=1}^{\infty} \frac{1}{[K_{j,j} : \mathbf{Q}]}\operatorname{li} x + O\left(\frac{x}{\log x \log\log x}\right). \tag{3.6}$$

同様に

$$\sum_{j \geq 1} \sharp\{p \leq x\ ;\ p \equiv 1 \pmod{q^{j+1}},\ q^j | I_a(p)\} = \sum_{j=1}^{\infty} \frac{1}{[K_{j+1,j} : \mathbf{Q}]}\operatorname{li} x + O\left(\frac{x}{\log x \log\log x}\right). \tag{3.7}$$

ここで, $[K_{j+1,j} : \mathbf{Q}] = q^{2j}(q-1)$ であることから, (3.1) 式にもどれば,

$$\begin{aligned}\sharp Q_a(x; q, 0) &= \left\{\frac{1}{\varphi(q)} - \sum_{j=1}^{\infty}\left(\frac{1}{[K_{j,j}^{(q)} : \mathbf{Q}]} - \frac{1}{[K_{j+1,j}^{(q)} : \mathbf{Q}]}\right)\right\}\operatorname{li} x + O\left(\frac{x}{\log x \log\log x}\right) \\ &= \frac{q}{q^2-1}\operatorname{li} x + O\left(\frac{x}{\log x \log\log x}\right) \quad (x \to \infty).\end{aligned} \tag{3.8}$$

こうして定理 2.2 が得られる.

上の証明では区間 $(0, x]$ を 3 つに分けて, 各区間上の和を違う方法で評価したが, その理由は, 素イデアル定理は剰余項が比較的大きく, 素イデアル定理だけを用いて正直に足すと, 剰余項の和が主要項を追い越してしまうからである.

注 意. 定理 2.2 において仮定されている条件 $a > 2$, a: square free は, 実はそれほど本質的ではない (定理 2.3 (i) も同じ). 実際, (3.8) 式に現れる種々の拡大次数を計算すれば, 一般の a についても $Q_a(x; q, 0)$ の密度を計算することができる. そして, これらの拡大次数の計算も難しい問題ではない (Moree [5, Lemma 2] または Murata [6, Section 3]). 例えば $a = 2$, $k = 2$ の場合, $Q_2(x; 2, 0)$ の密度は 17/24 であることが証明できる.

4 証明の概略 (2) — conditional cases

この節では, 定理 2.3(ii) の証明を述べる. 問題としては見かけ上 $k=q$: 素数, $l=0$ のときと変わらないようであるが, 証明は格段に難しくなる. そして現在のところこの場合には, GRH が必要である. この場合に GRH が必要なのは, 分解後の集合に代数体の素イデアル定理を適用して評価するときに, 「よりたくさんの」体に関して和をとる必要があり, unconditional な素イデアル定理では, 剰余項の和が主要項を追い越してしまうからである. また, この定理では a に $a\equiv 1 \pmod 4$ という条件がついているが, その他の a に対する密度計算はできていない. 数値実験の結果では, $a\not\equiv 1 \pmod 4$ の場合, 上の定理と同様, 1/6 づつに収束しそうなもの, 別の値に収束しそうなものの両方があり, これらの場合に密度を計算することは今後の課題である.

証明の方針は, まず $\sharp Q_a(x;4,l)$ $(l=1,3)$ を $\delta_l\cdot \mathrm{li}\, x+O(...)$ の形に書く. これは基本的に Murata [6] の議論と同じであるが, 上の体で完全分解しない素数を数えるために Chebotarev の密度定理を使う点が新しいところである. またこの過程では, これまでに剰余項つきで自然密度が求められていなかった新しい素数集合も登場し, その評価も新しい内容の一つである.

主要項の係数 δ_l はかなり複雑な級数であり, 直接値を求めることが, 今のところできない. しかし $\delta_1=\delta_3$ がわかれば, $Q_a(x;4,0)$ と $Q_a(x;4,2)$ の密度 (すなわち漸近式の主要項係数) はどちらも 1/3 であるから,

$$2\cdot\frac{1}{3}+\delta_1+\delta_3=1$$

となり, これから $\delta_1=\delta_3=1/6$ となって定理を得る. 実は a に関する条件 $a\equiv 1 \pmod 4$ は $\delta_1=\delta_3$ が示せるために必要な条件である.

まず問題の素数集合 $Q_a(x;4,l)$ を前節と同様に分解する. すると

$$Q_a(x;4,1) = \bigcup_{f\geq 1}\{S_a(x,f;1,1)\cup S_a(x,f;3,3)\}, \tag{4.1}$$

$$Q_a(x;4,3) = \bigcup_{f\geq 1}\{S_a(x,f;1,3)\cup S_a(x,f;3,1)\}, \tag{4.2}$$

ただし

$$S_a(f,x;i,j):=\{p\leq x;\ p\equiv 1+i\cdot 2^f \pmod{2^{f+2}}, I_a\equiv j\cdot 2^f \pmod{2^{f+2}}\}.$$

この集合の条件で, p の合同条件の右辺が 1 でないこと, I_a の合同条件の右辺が 0 でないことが, 問題を難しくしている主な原因である. $S_a(f,x;i,j)$ はさらに

$$S_a(f,x;i,j)=\bigcup_{l\geq 0}\{p\leq x;\ p\equiv 1+i\cdot 2^f \pmod{2^{f+2}}, I_a=(j+4l)\cdot 2^f\} \quad (i,j\in\{1,3\}) \tag{4.3}$$

と分解できるので,

$$N_a^{(k)}(x;s,t):=\{p\leq x;\ p\equiv s \pmod t, I_a=k\} \tag{4.4}$$

$(k=(j+4l)\cdot 2^f,\ s=1+i\cdot 2^f,\ t=2^{f+2})$ の密度がわかればよい. 実はこれから p の合同条件を除いた集合

$$N_a^{(k)}(x):=\{p\le x;\ I_a=k\}$$

の自然密度は Murata [6] において剰余項付きで計算されている.

定 理 4.1 (Murata) $a\in\mathbf{N}$, $a\ge 2$, square free, $k\in\mathbf{N}$ とすると, GRH のもとで

$$\sharp N_a^{(k)}(x)=\frac{k_0}{\varphi(k_0)}\sum_{d|k_0}\frac{\mu(d)}{d}\sum_{n=1}^{\infty}\frac{\mu(n)}{[G_{n,kd}:\mathbf{Q}]}\operatorname{li}x+O\left(\frac{x(\log\log x)^2}{\log^{3/2}x}\right), \tag{4.5}$$

ただし

$$k_0=\prod_{\substack{p|k\\ p:\text{ prime}}}p\quad(\text{これは } k \text{ の core と呼ばれる}),\quad G_{n,kd}=\mathbf{Q}(\zeta_n,\zeta_{kd},a^{1/kn}).$$

O の含む定数は a のみに依存する.

我々の集合 $N_a^{(k)}(x;s,t)$ は, この $N_a^{(k)}(x)$ に条件

$$p\equiv s\ (\mathrm{mod}\ t)\quad(s=1+i\cdot 2^f, t=2^{f+2})$$

を付け加えたものである. このような条件は, 円分体 $\mathbf{Q}(\zeta_t)$ での p の分解を考えることにより扱うことができる:

補 題 4.2 $\sigma_i\in\mathrm{Gal}(\mathbf{Q}(\zeta_t)/\mathbf{Q})$ を $\sigma_i:\zeta_t\mapsto\zeta_t^s$ で定まるものとする (i は s の定義に含まれるもの). すると,

$$p\equiv s\ (\mathrm{mod}\ t)\ \Leftrightarrow\ (p,\mathbf{Q}(\zeta_t)/\mathbf{Q})=\{\sigma_i\}.$$

しかし, $s\neq 1$ なので p は $\mathbf{Q}(\zeta_t)$ で完全分解しない. よってこれまでのように x 以下の素イデアルの個数を拡大次数で割るという単純な方法は通用しない. しかし, p の条件は Frobenius 写像を用いて書けるので, Chebotarev の密度定理が適用できそうである. 実際, 定理 4.1 の $G_{n,kd}$ のかわりに体

$$\tilde{G}_{n,kd}:=K_k(\zeta_n,\zeta_{kd},a^{1/kn},\zeta_t)$$

と次の条件をみたす $\sigma_i^*\in\mathrm{Gal}(\tilde{G}_{n,kd}/K_k)$ を考える:

$$\begin{cases}1^\circ\ \ \sigma_i^*\ \text{は}\ \zeta_n,\zeta_{kd},a^{1/kn}\ \text{を固定}\\ 2^\circ\ \ \sigma_i^*|_{\mathbf{Q}(\zeta_t)}=\sigma_i\end{cases} \tag{4.6}$$

このような σ_i^* はいつでも存在するとは限らないが, 存在すればただ1つであることが証明される. そこで $i=1,3$ に対して

$$c_i(n)=\begin{cases}1, & \sigma_i^*\ \text{が存在するとき},\\ 0, & \text{その他}\end{cases}$$

としておく. さらに, 集合

$$B(a^{1/k};K_k;x;m;s,t):=\left\{\begin{array}{l}\mathfrak{p}:\ K_k\ \text{の1次の素イデアル},\\ N\mathfrak{p}\le x, N\mathfrak{p}\equiv 1\ (\mathrm{mod}\ m),\\ a^{1/k}\ \text{は}\ \mathrm{mod}\ \mathfrak{p}\ \text{で原始根},\\ N\mathfrak{p}=p\equiv s\ (\mathrm{mod}\ t)\end{array}\right\}$$

を導入すれば, Murata [6] と同様にして

$$\sharp N_a^{(k)}(x;s,t)=\frac{1}{[K_k:\mathbf{Q}]}\frac{k_0}{\varphi(k_0)}\sum_{d|k_0}\frac{\mu(d)}{d}\sharp B(a^{1/k};K_k;x;kd;s,t) \tag{4.7}$$

が, さらに (剰余項はここでは省略するが)

$$\sharp B(a^{1/k};K_k;x;kd;s,t)$$

$$\sim\sum_{n=1}^{\infty}\mu(n)c_i(n)\sharp\{\mathfrak{p}:K_k\ \text{の素イデアル}, (\mathfrak{p},\tilde{G}_{n,kd}/K_k)=\{\sigma_i^*\}, N\mathfrak{p}\le x\} \tag{4.8}$$

が得られる. 最後の式の右辺の集合は Chebotarev の定理で評価できる. ただしここでも剰余項の大きさの都合により, GRH を仮定したものを用いる:

定 理 4.3 (Chebotarev density theorem) L/K: Galois 拡大, C を $G=\mathrm{Gal}(L/K)$ の共役類, d_L : L の判別式, $n_L=[L:\mathbf{Q}]$ とし,

$$\pi_C(x,L/K):=\{\mathfrak{p}:K\ \text{の素イデアル}, L\ \text{で不分岐}, (\mathfrak{p},L/K)=C, N\mathfrak{p}\le x\}$$

とすると, GRH のもとで

$$\pi_C(x,L/K)=\frac{\sharp C}{\sharp G}\mathrm{li}\,x+O\left(\frac{\sharp C}{\sharp G}\sqrt{x}\log(d_Lx^{n_L})+\log d_L\right)\quad(x\to\infty).$$

証 明. Lagarias-Odlyzko [3, Theorem 1.1]. ∎

これで $\sharp B(a^{1/k};K_k;x;kd;s,t)$ の評価ができ, (4.7) について次が得られる:

定 理 4.4 GRH のもとで

$$\sharp N_a^{(k)}(x;s,t)=\frac{k_0}{\varphi(k_0)}\sum_{d|k_0}\frac{\mu(d)}{d}\sum_{n=1}^{\infty}\frac{\mu(n)c_i(n)}{[\tilde{G}_{n,kd}:\mathbf{Q}]}\mathrm{li}\,x+O\left(\frac{x}{\log^2 x}(\log\log x)^4\right). \tag{4.9}$$

n に関する和は絶対収束する.

これで $N_a^{(k)}(x;s,t)$ の密度が剰余項付きで求まった (本節最初に述べた「これまでに剰余項つきで自然密度が求められていなかった新しい素数集合」がこれである).

注 意. ただし, $N_a^{(k)}(x;s,t)$ の密度そのもの, つまり漸近式の主要項係数のみであれば, Lenstra によってすでに求められていた ([4] の (2.15) 式および p.217 参照). しかし Lenstra [4] では基本的に解析密度の形で議論が進められており, 自然密度の場合の剰余項を与えることは本質的に不可能な証明となっている. したがって, われわれの定理 4.4 は決して Lenstra の自明な corollary ではない.

以上の結果を用いて, 少々複雑な剰余項の処理を経ると, 次の結果を得る:

定 理 4.5 $k^{(1)}=(1+4l)\cdot 2^f$, $k^{(3)}=(3+4l)\cdot 2^f$, $k^{(j)}$ の core を $k_0^{(j)}$ とする. a: square free のとき GRH のもとで, $r=1,3$ に対し,

$$Q_a(x;4,r)=\delta_r\cdot \operatorname{li} x+O\left(\frac{x}{\log x(\log\log x)^{5/2}}\right),$$

$$\begin{aligned}\delta_1 &= \sum_{f\geq 1}\sum_{l\geq 0}\frac{k_0^{(1)}}{\varphi(k_0^{(1)})}\sum_{d\mid k_0^{(1)}}\frac{\mu(d)}{d}\sum_n{}'\frac{\mu(n)c_1(n)}{[\tilde{G}_{n,k^{(1)}d}:\mathbf{Q}]}\\ &\quad+\sum_{f\geq 1}\sum_{l\geq 0}\frac{k_0^{(3)}}{\varphi(k_0^{(3)})}\sum_{d\mid k_0^{(3)}}\frac{\mu(d)}{d}\sum_n{}'\frac{\mu(n)c_3(n)}{[\tilde{G}_{n,k^{(3)}d}:\mathbf{Q}]},\end{aligned}\tag{4.10}$$

$$\begin{aligned}\delta_3 &= \sum_{f\geq 1}\sum_{l\geq 0}\frac{k_0^{(1)}}{\varphi(k_0^{(1)})}\sum_{d\mid k_0^{(1)}}\frac{\mu(d)}{d}\sum_n{}'\frac{\mu(n)c_3(n)}{[\tilde{G}_{n,k^{(1)}d}:\mathbf{Q}]}\\ &\quad+\sum_{f\geq 1}\sum_{l\geq 0}\frac{k_0^{(3)}}{\varphi(k_0^{(3)})}\sum_{d\mid k_0^{(3)}}\frac{\mu(d)}{d}\sum_n{}'\frac{\mu(n)c_1(n)}{[\tilde{G}_{n,k^{(3)}d}:\mathbf{Q}]}.\end{aligned}\tag{4.11}$$

ただし, $\sum_n{}'=\sum_{n\geq 1,n:\text{square free}}$ とする.

さて, $\delta_1=\delta_3$ を示すのがこのあとの目標だが, (4.10), (4.11) はいずれもかなり複雑な式で, 現在のところ直接値を求めることが困難である. そこで「係数比較」を行う. つまり (4.10) と (4.11) が実は同じものであることを示せば, 第 4 節で述べた通り, $\delta_1=\delta_3=1/6$ が得られる.

命 題 4.6 a: square free とする. $a\equiv 1 \pmod 4$ ならば, 任意の $n\geq 1$, square free に対して

$$c_1(n)=c_3(n).$$

これによって (4.10), (4.11) の 2 つの級数は同じものであることがわかり, 目標の定理 2.3 (ii) が得られる. つまり, $a\equiv 1 \pmod 4$ という条件は, 係数比較で密度が等しいことが証明できるために (現在のところ) 必要な条件である. したがってこれは技術的な問題とも言えるが, 数値実験の結果を見ると, かなり本質にかかわっている問題であるとも言える.

5 数値実験

自然数 a $(a\neq 1)$ を固定し, $k,l\in\mathbf{Z}$, $0\leq l<k$ をとる. このとき, いくつかの a,k に対して, $Q_a(x;k,l)$ の密度, すなわち $\sharp Q_a(x;k,l)/\pi(x)$ を計算した. x としては 10^7 まで取り, 10^3 から始めて 10 倍ごとに密度を出してある.

計算機環境

プログラムは C 言語で書き, OS は Linux (Kernel 2.0.36), コンパイラは GCC, CPU は Pentium 233MHz. 10^7 以下の素数は 664579 個あり, それらに対する位数 $D_a(p)$ の計算に要した時間は各 a につき約 7 時間 10 分〜30 分であった.

まず, 定理 2.2 に対応する場合, すなわち unconditional に密度が求まる場合を見るため, $a=10$, $k=q$: 素数として, $\sharp Q_{10}(x;q,0)/\pi(x)$ の表を掲げる. 表の最下段は「理論値」である $q/(q^2-1)$ の近似値である.

表 5.1 $Q_{10}(x;q,0)$ の密度

x	$q=2$	$q=3$	$q=5$	$q=7$
10^3	0.656627	0.349398	0.210843	0.144578
10^4	0.667482	0.376528	0.215159	0.143439
10^5	0.666736	0.375495	0.206778	0.144317
10^6	0.666607	0.375841	0.207616	0.145727
10^7	0.666833	0.374971	0.208539	0.145885
$q/(q^2-1)$	0.666667	0.375000	0.208333	0.145833

次に $a=2$, $k=q$: 素数の場合の $\sharp Q_2(x;q,0)/\pi(x)$ の値を示す. これは本稿では直接は扱っていないが, unconditional に密度を求めることが可能である (第 3 節最後の注意を参照). 以下のうち, $Q_2(x;2,0)$ の密度の理論値は 17/24, 他は $q/(q^2-1)$ である.

表 5.2 $Q_2(x;q,0)$ の密度

x	$q=2$
10^3	0.700599
10^4	0.714984
10^5	0.708372
10^6	0.707670
10^7	0.708168
$17/24\approx 0.708333$	

x	$q=3$	$q=5$	$q=7$
10^3	0.371257	0.203593	0.149701
10^4	0.377036	0.205212	0.144137
10^5	0.376395	0.209884	0.145866
10^6	0.375186	0.208581	0.145776
10^7	0.375256	0.208222	0.145808
$q/(q^2-1)$	0.375000	0.208333	0.145833

最後に, mod 4 での分類をいくつか見てみよう. この場合, $l=0,2$ のときは $Q_a(x;4,l)$ の密度は 1/3 づつであることが unconditional に解ける. しかし $l=1,3$ のときは, $a\equiv 1 \pmod 4$ ならば $Q_a(x;4,l)$ の密度は 1/6 づつであることが GRH の仮定のもとで証明できるが, a がこの合同条件を満たさないときの密度は今のところ不明である. 以下の表は, $a=5,3,6$ に対する $\sharp Q_a(x;4,l)/\pi(x)$ の値である. これらのうち, $l=1,3$ に関しては, $a=5$ が本稿定理 2.3 の (ii) で扱った場合である. その他の a に対する $Q_a(x;4,l)$ $(l=1,3)$ の密度の理論値は不明だが, $a=3$ のときは 1/6 に近い値であることが観察される. 一方, $a=6$ のときは 1/6 ではないと予想させる結果となっており, $a\equiv 1 \pmod 4$ という条件が問題の本質にかなり深くかかわっていることを窺わせるものと言える.

表 5.3 $Q_5(x;4,l)$ の密度

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.319277	0.156627	0.349398	0.174699
10^4	0.327628	0.167074	0.340668	0.164629
10^5	0.334619	0.167049	0.333055	0.165276
10^6	0.333227	0.167155	0.332934	0.166684
10^7	0.333320	0.166771	0.333099	0.166810

表 5.4 $Q_3(x;4,l)$ の密度

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.331325	0.150602	0.331325	0.186747
10^4	0.331703	0.163814	0.339038	0.165444
10^5	0.334411	0.167362	0.332325	0.165902
10^6	0.332488	0.166607	0.333762	0.167142
10^7	0.333298	0.166757	0.333397	0.166548

表 5.5 $Q_6(x;4,l)$ の密度

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.331325	0.126506	0.325301	0.216867
10^4	0.334963	0.133659	0.333333	0.198044
10^5	0.333785	0.133577	0.332847	0.199791
10^6	0.333151	0.132249	0.333507	0.201093
10^7	0.333331	0.132179	0.333019	0.201471

付 記. 定理 2.2 に関しては, Hasse [1], [2], Odoni [9] において, すでに同様の結果が得られていることが最近判明した.

参考文献

[1] Hasse, H. : Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $l \neq 2$ teilbarer bzw. unteibarer Ordnung mod p ist, Math. Ann. **162** (1965), 74-76.

[2] Hasse, H. : Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod p ist, Math. Ann. **166** (1966), 19-23.

[3] Hooley, C. : On Artin's conjecture, J. Reine Angew. Math. **225** (1967), 209-220.

[4] Ihara, Y. : Unpublished manuscript.

[5] Lagarias, J. C. and Odlyzko, A. M. : Effective versions of the Chebotarev density theorem, in *Algebraic Number Fields (Durham, 1975)*, 409-464, Academic Press, London, 1977.

[6] Lenstra Jr., H. W. : On Artin's conjecture and Euclid's algorithm in global fields, Invent. Math. **42** (1977), 201-224.

[7] Moree, P. : Uniform distribution of primes having a prescribed primitive root, preprint.

[8] Murata, L. : A problem analogous to Artin's conjecture for primitive roots and its applications, Arch. Math. **57** (1991), 555-565.

[9] Odoni, R. W. K. : A conjecture of Krishnamurthy on decimal periods and some allied problems, J. Number Theory **13** (1981), 303-319.

[10] 富澤 一夫『素数の周期による分類』, サイエンティスト社 (1988).